Exhibit 1

Philip A. Werlau Expert Disclosure

<u>Expert Disclosure – Philip A. Werlau</u>
(February 14, 2025)

Philip A. Werlau is a Senior Investigator at Anchain.AI. He has been a Senior Investigator since January 2025, and prior to that his title was Engineering Manager and Senior Smart Contract Security Researcher. He will be called to testify regarding blockchain technology, smart contracts, and internet applications, as further described below.

A. Qualifications and Prior Testimony

Mr. Werlau has been employed at Anchain.AI since December 2021, where he leads blockchain and smart contract investigations for various government agencies, including IRS-Criminal Investigations, the Securities and Exchange Commission, and for private customers. He managed a team in the design and development of Web3SOC, an application used for Web3 incident response. His experience has included leading multiple investigations into cryptocurrency transactions related to hacking and money laundering, conducting smart contract code audits for government institutions and large blockchain companies, and leading the development of an Ethereum non-fungible token (NFT) platform and associated web storefront, where he developed multiple smart contracts as well as the web-based user interface and the back-end system that supported the platform.

Prior to working at Anchain, Mr. Werlau was a software developer from 2007 through 2014. In that capacity, he was a full-stack software developer dealing with web development, database management, development of Javascript interfaces, among other duties. He also previously worked for a network security company in penetration testing, in which capacity he developed tools for threat assessment and vulnerability detection. From 2016 through 2021, he worked at a security operations center, working in network security. His title from 2019 through 2021 was senior security engineer, with duties including managing a security information and event management (SIEM) system, making security alerts, and building support for new devices or vendors.

B. Anticipated Opinions

Outlined below are the opinions that Mr. Werlau is expected to offer, which are based on his training and experience working in blockchain and smart contract investigations, as well as specific bases and reasons for those opinions listed below:

1.   Ether ("ETH") is a decentralized form of electronic currency, or cryptocurrency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a "peer to peer" network. ETH transactions are processed collectively by the computers composing the network, which are referred to as "nodes."

2.   To acquire ETH in the first instance, a user typically purchases it from an ETH "exchange." In return for a commission, ETH exchanges accept payments of currency in some conventional form (cash, wire transfer, or otherwise), or payments of another type of cryptocurrency, and exchange the money for a corresponding number of ETH, based on a

1

fluctuating exchange rate. Exchanges also accept payments of ETH and exchange the ETH back for conventional currency or another type of cryptocurrency, again charging a commission for the service.

3.   Once a user acquires ETH, the ETH is stored as a balance in an Ethereum "address," designated by a hexadecimal string of letters and numbers. The Ethereum address is analogous to the account number for a bank account. A private key is similar to a PIN or password that allows a user the ability to access and transfer value associated with the Ethereum address. Once an Ethereum user funds an address with ETH, the user can then use the ETH to conduct financial transactions, such as transferring ETH to other addresses. A transfer of ETH is conducted by transmitting an instruction to a node on the Ethereum network, which then announces the transfer to the other nodes on the Ethereum network. To validate the transfer, the Ethereum network charges what is known as a "gas" fee, which is a fee paid in ETH to the nodes that operate the Ethereum blockchain, which covers their costs of doing so. Thus, to conduct a transaction on the Ethereum blockchain, an Ethereum address must have enough ETH to cover the gas fee charged by the Ethereum network for the transaction.

4.   All ETH transactions are recorded on a public ledger known as the "Ethereum blockchain," which is stored on the nodes that make up the Ethereum peer-to-peer network. The Ethereum blockchain records the balance held in each Ethereum address and records all ETH transactions between Ethereum addresses, including a block number associated with the transaction that can be used to identify the date and time of the transaction. This public ledger serves to prevent any user from spending more ETH than the user holds in his or her Ethereum address. The public nature of the Ethereum blockchain also means that the movement of funds over the Ethereum blockchain can be traced. However, the Ethereum blockchain only reflects the movement of funds between anonymous or pseudonymous Ethereum addresses and therefore cannot by itself be used to determine the identities of the persons involved in the transactions.

5.   The Ethereum blockchain also stores computer programs known as "smart contracts." A smart contract is a computer application hosted on the Ethereum blockchain that can hold ETH in an Ethereum address and release it when the smart contract receives instructions that comply with the smart contract's code. A smart contract can also communicate with other smart contracts to receive information from those smart contracts or instruct those smart contracts to conduct a function. The Ethereum blockchain stores all transactions and balances associated with smart contracts. All of the above-described testimony about ETH and the Ethereum blockchain is based on Mr. Werlau's years of experience studying and using the Ethereum blockchain and publicly available information and documentation regarding the Ethereum blockchain, including the Ethereum white paper and other explanatory documentation available at Ethereum.org.

6.   Mr. Werlau will provide an overview of the Tornado Cash service as it existed from its inception in 2019 through in or about August 8, 2022. Unless otherwise noted below, this is the relevant date range for the descriptions contained in this disclosure. The Tornado Cash service was a cryptocurrency mixer. The term "mixer" does not have a technical definition, but it is used here to refer to a service that accepts cryptocurrency deposits from multiple customers, mixes or commingles those deposits in some way, and then transmits those deposits to new cryptocurrency addresses for its customers. The general purpose of a cryptocurrency mixer is to enable its customers to move cryptocurrency from one address to another address without a connection

2

between the two addresses on the public blockchain. The Tornado Cash service primarily operated on the Ethereum blockchain and combined multiple features to provide this mixing service and conceal the connection between customer deposits and withdrawals, including but not necessarily limited to the following:

a. Customer deposits and withdrawals could only be made in certain fixed amounts. For instance, the Tornado Cash ETH service only allowed deposits and withdrawals in amounts of 0.1, 1, 10, and 100 ETH, and there were individual smart contracts for each ETH increment (the "Tornado Cash pools"). This made it more difficult to link particular deposits and withdrawals, because the public Ethereum blockchain transactions for each of the Tornado Cash pools would show nothing but a uniform stream of deposits and withdrawals of the same amount of ETH.

b. The Tornado Cash service had a graphical user interface (the "UI") and a command line interface (the "CLI") that calculated and provided customers with a unique secret note associated with each deposit. Because the UI and the CLI generated the note, they could have been initially designed to store the note in a centralized location in a manner that was accessible to the operators of the Tornado Cash service. The UI and CLI could also have been modified at any time to implement this change, but that design choice was never implemented. The UI and the CLI also each had a function that used the secret note as an input to generate a unique zero-knowledge proof that could be used to make a withdrawal. A zero-knowledge proof is a cryptographic protocol that allows a person to prove knowledge of something—in this case, the secret note associated with a particular deposit—without disclosing the secret note itself. Generation of this proof involved complex mathematics and would have required a high level of technical sophistication to do without using the UI or the CLI.

c. The Tornado Cash service made the UI accessible to customers through a normal website that was accessible using any standard web browser. This enabled anyone using a standard computer or cellphone to use the Tornado Cash service, which increased the pool of potential users of the Tornado Cash service. Because mixers operate on the principle of commingling customer deposits, a service that is accessible to a broader group of people will provide more anonymity for its customers than one that is accessible to a narrower group of people.

d. The Tornado Cash service provided a network of "relayers" to actually transmit the instructions for Tornado Cash withdrawals to the Ethereum blockchain. As detailed below, a Tornado Cash customer could request that a relayer conduct a withdrawal of ETH that the customer had deposited into the Tornado Cash pools. The relayer for a withdrawal would pay the gas fees associated with the withdrawal and receive a portion of the withdrawal as a fee for providing this service. This provided enhanced anonymity for customers because without a relayer, a customer of the Tornado Cash

3

service seeking to withdraw ETH would have needed to use an address that already contained a balance of ETH to conduct the withdrawal, so the customer could pay the gas fee. The transaction that funded that address could potentially be traced on the blockchain. With a relayer, on the other hand, the customer could withdraw to a new Ethereum address that had no prior transaction history.

e. The default setting for the Tornado Cash UI was to have the UI select the relayer for customers, allowing customers to avoid the risk that any particular patterns could be detected if they selected their own relayers. The relayer selection function was originally performed entirely by the UI itself, based on a list of relayers included within the UI. In or around February 2022, however, the Tornado Cash service deployed a new smart contract (the "Relayer Registry"). The UI would read the list of relayers in the Relayer Registry and run an algorithm encoded within the UI (the "relayer algorithm") to select the relayer for each withdrawal.

f. The Tornado Cash website provided customers with instructional documents regarding additional measures they could take to conceal their identity, including using Tor and/or a VPN, which are both methods for concealing the user's Internet Protocol ("IP") address, when making deposits and withdrawals, deleting data from their web browsers, and extending the amount of time between deposits and withdrawals to further obscure the connection. At at least some times, the Tornado Cash website also displayed the customers' IP address and geolocation as it was received by the website, apparently to remind them to use a VPN or other method to conceal their true IP address.

This overview is based on a review of the Tornado Cash website, UI, CLI, the code underlying these applications as maintained in Github repositories, the code for various smart contracts associated with the Tornado Cash service, and instructional and informational documents posted by the Tornado Cash founders or other participants in the Tornado Cash service to docs.tornado.cash or Medium.

7.   On the Internet, a domain name is used to identify ownership and control of a website. A user can register a domain name through a number of private companies, and can then host content accessible on the web at that domain name. The domain name tornado.cash was registered with Google in July 2019, and was paid for by Roman Storm. By virtue of this registration, Roman Storm, Roman Semenov, and Alexey Pertsev (collectively, the "Tornado Cash founders") controlled that domain name and had the ability to decide what content was provided to users who visited that domain name. Google billing records for Tornado Cash show that the service was billed to Roman Storm at an address in Seattle, Washington, with a credit card in Storm's name tied to the account. The website associated with the tornado.cash domain was hosted on Amazon Web Services ("AWS") from at least June 2020 through around August 8, 2022. AWS account information for the tornado.cash website hosting show that the hosting service was billed to Alexey Pertsev. This testimony will be based on a review of archived versions of the tornado.cash website from the Internet Archive's Wayback Machine, communications between

4

Storm, Semenov, and Pertsev, subpoena returns from Google and AWS, and a domain name registry report for tornado.cash.

8.   The tornado.cash website included a link to a website called docs.tornado.cash. This website provided a repository of documents hosted on Github that explained the Tornado Cash service, how to use the service, and provided advice on using the service while concealing the user's identity. This testimony will be based on explanatory documents posted on the tornado.cash website and the docs.tornado.cash repository, and from a review of Github records.

9.   The tornado.cash website linked to the Tornado Cash UI, a web application that allowed customers of the Tornado Cash service to make deposits and withdrawals. The Tornado Cash UI could be accessed using the ENS domain name tornadocash.eth. ENS is the Ethereum Name Service, which is a naming protocol similar to a web domain registered using the domain name service. The owner of an ENS domain can direct traffic from that domain to a blockchain address or to other content posted by the owner, using a hash to identify where that content is hosted. Most ordinary web browsers cannot access a .eth domain, so the Tornado Cash website provided a link to a portal called eth.limo, as well as alternative portals, which allowed customers to access the UI at the tornadocash.eth ENS domain using a standard web browser. Just as with a traditional website, a user can register an ENS domain name and can then control what content is accessible at that ENS domain name. The domain name tornadocash.eth was registered on or around August 7, 2019, and the Ethereum address used to register the domain name was the blockchain address designated by the ENS domain poma.eth. That address is attributable to Roman Semenov. From the time of its registration until on or around August 8, 2022, the tornadocash.eth domain name was under the control of Roman Semenov, meaning that he, and anyone he decided to share control with, had the ability to control what contents were delivered to visitors at that domain name. The content that was hosted at tornadocash.eth was the Tornado Cash UI. The UI that was accessible at the tornadocash.eth domain was regularly modified and updated until around August 8, 2022, including the particular revisions discussed in more detail below. This testimony will be based on Ethereum blockchain records associated with tornadocash.eth, a review of versions of the UI that were accessible at that domain name at various points in time obtained from Pinata, and a review of communications between the Tornado Cash founders.

10.   Instead of being hosted on a traditional web server, the Tornado Cash UI was hosted on a peer-to-peer network called the Interplanetary File System ("IPFS"). From at least October 2020 through at least on or about August 8, 2022, the Tornado Cash UI was hosted on IPFS using a service called Pinata, through a Pinata account in the name of Alexey Pertsev. Pertsev shared the Pinata login information used to upgrade and modify the UI posted to IPFS with Storm and Semenov. Pinata provides IPFS nodes, which are computers for hosting contents on IPFS, and which provide Pinata users with assurance that their contents will be readily accessible to users with little or no downtime and minimal delay or lagging. Using the Pinata service allowed the Tornado Cash founders to post the UI to IPFS, and modify and upgrade the UI from time to time, while maintaining a consistent quality of service and accessibility that would be similar to the quality of service obtained from hosting content on a central server. This testimony will be based on a review of subpoena returns from Pinata, bank records, chats between Pertsev, Storm, and Semenov, information from the Ethereum blockchain, and publicly available information about IPFS and Pinata.

5

11.   The code for the Tornado Cash UI was available on a Github repository. The first commit, or update to the code, to this repository was from Roman Storm, and Storm made approximately 200 commits to the repository between on or around July 7, 2019, and on or around October 10, 2021. Prior to April 21, 2022, the code for the Tornado Cash UI was not made available to the public except in a form that was "minified," which involves stripping down the source code and changing certain elements within the code to make the overall file smaller. With respect to code for a website, such as the Tornado Cash UI, the purpose of minifying is to improve the performance of the website. With minified code, it becomes more difficult to reverse engineer the underlying source code or its history because, for example, the values of certain variables in the code are obscured in the minification process. This testimony will be based on Github records and the UI code repository maintained by Github under the name tornadocash/tornado-cash-ui.

12.   In addition to the UI, the Tornado Cash service had a CLI, which is a non-graphical interface (that is, an interface by which a user can communicate using text instructions rather than icons, windows, or menus) that could be downloaded and run on a customer's computer. Using the CLI required a degree of knowledge of computer code that was not required to use the UI, which had a more easily accessible graphical interface. The program for the CLI was developed in a Github repository that was created by Roman Storm. Roman Storm made approximately two commits to the CLI, and he also approved pull requests to update the master branch of the CLI code submitted by other developers on multiple occasions. This testimony will be based on Github records and the CLI code repository maintained by Github under the name tornadocash/tornado-cli.

13.   In or around December 2020, the Tornado Cash founders announced the creation of a new cryptocurrency token on the Ethereum blockchain, the TORN token. 10 million TORN tokens were minted. 30% were distributed to the Tornado Cash founders and investors in the Tornado Cash service, 5% were distributed to early customers of the Tornado Cash service, 10% to be distributed to customers who made deposits into the Tornado Cash service based on the amount of time they left the deposits in the service, which was designed increase the size of the pools by incentivizing customers to leave funds in the pools and correspondingly increase the anonymity of the service. The remaining 55% of TORN tokens were placed in treasury controlled by a smart contract, the Tornado Cash Governance smart contract, that was created around the same time. Holders of TORN tokens could deposit TORN tokens into the Governance smart contract, which would allow them to vote on various governance proposals. However, this announcement did not have any effect on the Tornado Cash founders' control over the website, the UI, or the tornadocash.eth domain. Later, on or about August 8, 2022, after the announcement of sanctions on Tornado Cash, the poma.eth address transferred ownership and control of the tornadocash.eth domain to the Tornado Cash Governance smart contract. After this transfer, control over the tornadocash.eth domain could be exercised by a majority vote of tokens deposited into the Tornado Cash Governance smart contract. This testimony will be based on a review of the announcement of the Tornado Cash TORN tokens and governance structure, and blockchain data concerning the tornadocash.eth domain.

14.   Although the original Tornado Cash pools were rendered unchangeable in or around May 2020, the other features of the Tornado Cash service could be and in fact were changed

6

from time to time. For instance, in or around December 2020, in connection with the announcement of the TORN tokens, the Tornado Cash founders implemented a smart contract that the Tornado Cash founders referred to as a "proxy," and modified the UI and CLI to send deposit and withdrawal requests to the "proxy" smart contract instead of interacting directly with the Tornado Cash pools. The first "proxy" contract operated from around December 2020 until around March 30, 2021. At that time, it was replaced with a new "proxy" smart contract that from around March 30, 2021 until around February 2022. These "proxies" were used to administer a program called anonymity mining, which rewarded customers with TORN tokens for leaving deposits in the Tornado Cash service for periods of time. Each of these "proxies" was disabled when it was replaced by a new "proxy" contract. This testimony will be based on a review of the announcement of the Tornado Cash TORN tokens and governance structure and other announcements made by the Tornado Cash founders, the computer code for the UI and CLI, and data from the Ethereum blockchain.

15.   There was a significant overhaul of the architecture of the Tornado Cash service in or around February 2022. The updated structure of the Tornado Cash service that was implemented in or around February 2022 involved a multi-step process for making deposits and withdrawals. This process involved significant changes to both the UI and the CLI and the deployment of a number of new smart contracts. The new smart contracts deployed in or around February 2022 included contracts referred to as the Tornado Cash Router, the Instance Registry, the Relayer Registry, the Fee Manager, and the Governance Staking contract. Implementing these smart contracts and a new design of the UI and the CLI created a new way for the Tornado Cash service to monetize its technology and for holders of TORN tokens to realize a share of the revenues generated by relayer fees. Between around February 2022 and around August 8, 2022, deposits and withdrawals in the Tornado Cash service worked as follows:

    a. When a customer used the UI to make a deposit, the UI would generate a secret note for the deposit, which would include identifying information about the type of cryptocurrency and the amount of the deposit and a unique string of numbers and letters, and provide that note to the customer. In addition, the UI would send the deposit request to the Tornado Cash Router. The Router would call the Instance Registry to verify that the pool selected by the customer was enabled. If it was, the Router would transmit the deposit data to the selected Tornado Cash pool, which would have the effect of announcing to the Ethereum blockchain a transfer of the selected amount of cryptocurrency from the customer's address to the Router and then to the pool that corresponded with the amount of the deposit. The deposit request would also include a hash derived from the secret note, which the Router would transmit to the relevant Tornado Cash pool. Deposits worked in essentially the same way for the CLI, except that the customer would have to input a text instruction to identify a node to be used to convey the deposit request to the Router.

    b. When a customer used the UI to make a withdrawal, the customer would enter the customer's secret note in the UI. The default setting of the UI would select a relayer to make the withdrawal, and the customer could

change the default to either make the withdrawal without a relayer, or to choose a particular relayer to make the withdrawal. As noted above, there were anonymity enhancing features of having the UI choose the relayer, and this was also the most accessible option for customers because it did not require the customer to have any information about which relayers were available. If the customer chose the default option of having the UI select the relayer, the customer's withdrawal request initiated a multi-step process:

i.   First, the UI would read the list of relayers that was stored in the Relayer Registry smart contract. The Relayer Registry was set up so that a relayer was required to obtain at least 300 TORN tokens and deposit, or "stake," them into the Governance Staking smart contract to be included in the list. After reading the Relayer Registry, the UI would run an algorithm that was added to the UI in or around February 2022, which would select a relayer to conduct the transaction.

ii. The UI would also run a function to generate a zero-knowledge proof based on the customer's secret note.

iii. After selecting a relayer and generating a proof, the UI would send the customer's withdrawal request, including the zero-knowledge proof, to the selected relayer.

iv. Upon receiving the withdrawal request, the relayer would transmit the request to the Tornado Cash Router to initiate the transaction on the Ethereum blockchain. The Router would then run several functions. It would call the Instance Registry to confirm that the selected Tornado Cash pool was enabled. It would then call the Relayer Registry, which would in turn call the Fee Manager, which would determine a commission in TORN tokens to be paid by the relayer. The commission paid by the relayer was calculated based on the price of TORN tokens in ETH, so that the amount of TORN tokens charged to the relayer was effectively a proportion of the amount of ETH earned by the relayer for the transaction. The Relayer Registry would then direct a transfer of ownership of the relayer's staked TORN tokens in the Governance Staking smart contract to the User Vault. The User Vault was controlled by the Tornado Cash Governance smart contract, which was controlled by a vote of the holders of TORN tokens who had staked tokens in the Governance smart contract. Those TORN token holders could vote on how to spend the proceeds from relayer commissions, including by distributing those proceeds among themselves or by using those proceeds to pay Tornado Cash business expenses.

v.   The Tornado Cash Router would then send the zero-knowledge proof which it had received from the relayer to the relevant Tornado

8

Cash pool, which would use a Verifier smart contract to verify the proof. Upon verification, the whole transaction would be announced to the Ethereum blockchain, resulting in the transfer of ETH to the withdrawal address designated by the customer and to the relayer selected to conduct the transaction. For a 100 ETH withdrawal, the relayer fees were typically in the neighborhood of 0.4 ETH, meaning that the customer would generally receive around 99.6 ETH and the relayer would receive around 0.4 ETH. The relayer would also pay the gas fees for the overall transaction.

vi. Withdrawals using the CLI followed a similar structure except that the CLI did not run the relayer algorithm, and thus did not select relayers for customers. Thus, to make a relayed withdrawal using the CLI, a customer had to select a relayer to conduct the transaction, and input a text instruction to identify that relayer. However, after the customer's withdrawal request was sent to the relayer using the CLI, the subsequent steps, and the smart contracts involved, were the same as for a relayed withdrawal using the UI.

This testimony will be based on a review of the code for the UI and the CLI and the code for the above-listed smart contracts.

16.   The February 2022 upgrade to the Tornado Cash architecture served to increase the value of TORN tokens in two ways. First, it required relayers to purchase TORN tokens, creating increased market demand for these tokens. To be included in the Relayer Registry, relayers had to obtain and deposit, or "stake," at least 300 TORN tokens in the Governance Staking smart contract. In addition, because the relayer algorithm encoded in the UI selected relayers in part on the basis of how many TORN tokens they had staked, relayers had an incentive to purchase even more tokens. And, because relayers had to pay a commission in TORN tokens out of the TORN tokens they had staked in the Governance Staking smart contract each time they conducted a withdrawal for a customer, they had an ongoing requirement to purchase more TORN tokens to maintain their position in the Relayer Registry. Second, the implementation of the commission model for relayers meant that purchasers of TORN tokens could realize an ongoing revenue stream by staking TORN tokens in the Governance smart contract, where they would receive a share of the commissions earned from the relayers. This testimony will be based on a review of the code for the UI and the CLI and the code for the above-listed smart contracts.

17.   The changes to the Tornado Cash service in February 2022 demonstrate that the Tornado Cash founders were able to make these and similar changes during the relevant time period. Because the Tornado Cash founders had control over the UI and the CLI, they could make many of these changes based on their own decision, including by deciding which smart contracts the UI and CLI would interact with in the course of executing a Tornado Cash transaction. Indeed, even though the original Tornado Cash pools were immutable after May 2020, the Tornado Cash founders could have created new pool smart contracts at any time, and updated the Tornado Cash UI and CLI to interact with those new pools. In addition, while some aspects of the Tornado Cash service, such as the Proxy smart contract that existed before February 2022, were controlled by the Governance smart contract, the Tornado Cash founders had the ability to make proposals for

9

changes even to those features to the participants in the Governance smart contract. This testimony will be based on a review of the code for the UI and the CLI and the code for the above-listed smart contracts, a review of communications among the Tornado Cash founders, as well as the opinions described above about the Tornado Cash founders' control of the UI and CLI and the tornadocash.eth domain where it was posted.

18.   The changes to the Tornado Cash service in February 2022 also demonstrate that the Tornado Cash founders could have included a know-your-customer ("KYC") function in the Tornado Cash service. For example, the February 2022 changes implemented the new Instance Registry and Relayer Registry smart contracts and the new Tornado Cash Router smart contract. When these were created, the Router was programmed to call the Instance Registry as part of each deposit, and to call both the Instance Registry and the Relayer Registry as part of each relayed withdrawal. This means that the Tornado Cash founders could also have implemented a new smart contract with a registry of authorized users, and could have programmed the Router to call that smart contract to check that the deposit address and/or withdrawal address were included on that list. This hypothetical smart contract could have been set up so that the Tornado Cash founders, or another person or entity, had the ability to add or remove authorized users based on a KYC process. There is no technical reason that the Tornado Cash service could not have been updated at any time to implement such a system. This testimony will be based on a review of the code for the UI and the CLI and the code for the above-listed smart contracts.

19.   There was also a change made to the Tornado Cash service on or around April 15, 2022. On or about that date, OFAC announced that a North Korean cybercrime organization, the Lazarus Group, was responsible for the Axie Infinity Ronin Network exploit which had resulted in the theft of approximately $625 million worth of cryptocurrency, and that a particular Ethereum address connected to the exploit was subject to United States sanctions. Following this announcement, the Tornado Cash founders implemented a change to the UI to have the UI call a smart contract called the Chainalysis Oracle before permitting deposits into the Tornado Cash service, to determine if the address making the deposit was on the sanctions list. The Tornado Cash founders could also have incorporated this change into the CLI, but did not do so. In addition, the Tornado Cash founders could have embedded this sanctions screen into the smart contract architecture of the service, but did not do so. For instance, just as the Tornado Cash service had been changed in February 2022 to implement calls by the Tornado Cash Router to the newly created Instance Registry and Relayer Registry, it could have been changed in April 2022 to implement a call by the Tornado Cash Router to the Chainalysis Sanctions Oracle or to implement other sanctions screening mechanisms. And, as noted above, the service could also have been changed to implement KYC processes, which would also have the effect of enabling more effective sanctions screening by providing information about who the customer initiating the deposit or withdrawal was. Embedding compliance tools into the architecture in this way would have made it more difficult for Tornado Cash customers to evade the minimal sanctions screening that was added to the UI in April 2022. This testimony will be based on a review of public information about OFAC's announcement of sanctions, chats among the Tornado Cash founders, and a review of the code for the UI and the CLI.

20.   As described above, the Tornado Cash UI interacted with the Ethereum blockchain in the course of making deposits and withdrawals. To carry this traffic between the UI and the

blockchain, the UI needed to use a designated node on the Ethereum blockchain. While there are free services available to handle limited traffic with the Ethereum blockchain, the amount of traffic generated by the Tornado Cash UI was too great to rely on those free services for reliable service to Tornado Cash customers. Accordingly, the UI used at least three services, provided by Infura, Alchemy, and The Graph, to handle the traffic. Bank records indicate that Roman Storm paid for the Infura and Alchemy services using a bank account in the name of Peppersec, Inc. This testimony will be based on a review of communications among the Tornado Cash founders, a review of invoices from Infura and Alchemy, and bank records.

21.   Based on data from the blockchains on which the Tornado Cash service operated, it is possible to identify the percentage of Tornado Cash withdrawals that used a relayer. During the period from September 1, 2020 through August 8, 2022, approximately 99% of all withdrawals from the Tornado Cash service used a relayer. This testimony will be based on blockchain data.

22.   When an address initiates a transaction on the Ethereum blockchain, the address also communicates the amount of gas that it is willing to use to complete the transaction, which is commonly referred to as the "gas limit." After the transaction is completed, the blockchain records information both about the gas limit that was initially set and the amount of gas that was actually used, which can be used to identify the "gas ratio" for the transaction. The gas limit and gas ratio can be used to determine whether different transactions likely originated using the same method, if they have the same or nearly the same gas limit and gas ratio. In the case of the Tornado Cash service, this method can be used to identify which deposits used the UI and which deposits used the CLI. The UI and the CLI both originally had a fixed gas limit in their computer code, but this limit was different for the UI and the CLI. Subsequently, the UI was changed to make an estimate of how much gas would be used in the transaction, and then add a fixed amount as a buffer to set the gas limit for the transaction. The CLI, by contrast, was changed to make an estimate of how much gas would be used in a transaction, and then multiply that estimate by a fixed amount to set the gas limit for the transaction. Thus, both the UI and the CLI have distinctive identifying characteristic gas limits and gas ratios that are visible on the blockchain, and those distinctive characteristics changed over time. An analysis of blockchain data for Tornado Cash deposits shows that approximately 96.2% of ETH deposits on the Ethereum blockchain from September 1, 2020 to August 8, 2022 used the UI, and approximately 2.8% of ETH deposits on the Ethereum blockchain from September 1, 2020 to August 8, 2022 used the CLI. This testimony will be based on blockchain data, and the code for the versions of the UI and CLI that existed at different points during this time period.

23.   In addition, Mr. Werlau will use the gas limit and gas ratio associated with certain Tornado Cash deposits identified by the Government's expert witness Joel DeCapua as being associated with particular criminal incidents, including the Ronin hack perpetrated by the Lazarus Group, and identify whether those limits and ratios indicate that particular deposits were made using the UI or CLI.
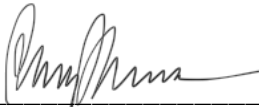
24.   The Tornado Cash service maintained a domain titled ip.tornado.cash, which would provide information about the IP address of the user accessing the Tornado Cash website and the UI. The code for the UI included an instruction for the UI to retrieve this information from ip.tornado.cash from in or about October 2020 through in or about March 2022. The Tornado Cash

11

website also used this information to display the user's IP address and the geolocation associated with that IP address. An IP address is a number used to identify users communicating over a network such as the Internet. Ordinarily, an IP address is communicated from a user's web browser to the web server, such as the host of a website, during every information request, and the website owner can keep records of the IP addresses used to visit the website at particular points in time. This testimony will be based on a domain name registry report for ip.tornado.cash, the Tornado Cash founders' initial public announcement of the Tornado Cash service, and the code for the UI.

25.   The Tornado Cash service provided customers with an optional feature referred to as the "compliance tool." The compliance tool allowed a customer of the Tornado Cash service to generate a report using a secret note to identify which deposit and which withdrawal corresponded to that secret note. This enabled customers of the Tornado Cash service to document their own transaction history if they chose to do so. However, the Tornado Cash service's "compliance tool" did not require customers to provide the Tornado Cash service with any identifying information, and did not enable the Tornado Cash service to engage in any transaction monitoring, recordkeeping, reporting, or other anti-money laundering compliance measures. The "compliance tool" was also entirely optional for customers of the Tornado Cash service. This testimony will be based on a review of instructional documents posted to the Tornado Cash website and a review of the code for the UI and CLI.

C. Approval and Signature

I hereby approve the disclosure of my qualifications, anticipated opinions, and bases for such opinions, as set forth above.

_____
Philip A. Werlau